REMARKS

Claims 1-6, 9-15, 17-38, 40-43, 45-51, 61, 62 and 64 remain pending in this application.

Initially, the applicant notes that the Final Office Action states that the applicant's amendment filed February 16, 2006 necessitated the new grounds of rejection (Final Office Action – page 15). The applicant respectfully disagrees and requests withdrawal of the finality of the current Office Action.

Claim 1 was amended in the response filed February 16, 2006 to incorporate the features of original claim 7. Claim 7 was rejected in the previous Office Action under 35 U.S.C. § 103(a) as being unpatentable over Goldstone (U.S. Patent Publication No. 2002/0101819; hereinafter Goldstone) in view of Khosravi (U.S. Patent Publication No. 2003/0039245). Current claim 1, which includes the features of original claim 7, is now rejected under 35 U.S.C. § 103(a) as being unpatentable over Goldstone in view of Fedyk et al. (U.S. Patent No. 6,560,654; hereinafter Fedyk). Therefore, the applicant asserts that the new grounds of rejection of claim 1 based on the combination of Goldstone and Fedyk was not necessitated by the amendment. In other words, changing the rejection of previous claim 7 based on the combination of Goldstone and Khosravi to the combination of Goldstone and Fedyk in current claim 1 was not necessitated by the previous amendment since current claim 1 merely incorporated the features of previous claim 7. Accordingly, withdrawal of the finality of the current Office Action is respectfully requested.

Claims 61, 62 and 64 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Chen et al. (U.S. Patent Publication No. 2002/0032854; hereinafter Chen). The rejection is respectfully traversed.

Claim 61 recites a method for responding to an attack that includes receiving attack information at a central management system from a first device via a network and managing a response to the attack at the central management system. Claim 61 also recites receiving, at the central management system, additional attack information from other devices via the network and communicating, by the central management system, information associated with the additional attack information to the first device.

The Final Office Action states that server 101 of Chen is equivalent to the central management system recited in claim 61 and attack host 113 is equivalent to the claimed first device (Final Office Action – page 3). The Final Office Action also states that Chen discloses managing a response to an attack at the central management system and that the central management system receives additional attack information from other devices and points to Fig. 2, elements 106, 107 and 109 along with paragraph 45, lines 1-24 of Chen for support (Final Office Action – page 3).

Fig. 2 of Chen illustrates an edge router 102 coupled to routers 103-111. Chen at paragraph 45 discloses that edge router 102 creates duplicate programs of itself and forwards these duplicate programs to routers 106, 107, 109 and 110. Routers 106, 107, 109 and 110 then stop traffic from attack hosts 113, 114, 116 and 117 from reaching server 101. Chen at

paragraph 45 further discloses that when the attack on server 101 has ended, the mobile packet filtering programs installed on routers 106, 107, 109 and 110 send the history log of the attack to the original mobile packet filtering program installed on edge router 102.

Chen, however, does not disclose or suggest that server 101, alleged to be equivalent to the central management system of claim 61, receives additional attack information from any of devices 106, 107 and 109, which are alleged to be equivalent to the other devices recited in claim 1. In contrast, routers 106, 107 and 109 merely forward attack logs to edge router 102 after the attack has ended. Routers 106, 107 and 109 clearly do not forward additional attack information to server 101, as would be required by claim 61 based on the alleged equivalence of the elements in Chen with the features recited in claim 61.

Claim 61 also recites communicating, by the central management system, information associated with the additional attack information to the first device. The Final Office Action states that Chen discloses this feature and points to paragraph 45, lines 1-24 for support (Final Office Action – page 3). As discussed above, Chen at paragraph 45 discloses that a mobile packet filtering program installed on edge router 102 is moved to routers 106, 107, 109 and 110 and that after an attack has ended, routers 106, 107, 109 and 110 sends a history log to edge router 102. This portion of Chen clearly does not disclose or suggest that server 101 receives additional attack information from routers 106, 107, 109 and 110, much less communicates information associated with the additional attack information to attack host 113, as would be

required by claim 61 based on the alleged equivalence of the elements in Chen with the features recited in claim 61.

For at least these reasons, Chen does not disclose or suggest each of the features of claim 61. Accordingly, withdrawal of the rejection and allowance of claim 61 are respectfully requested.

Claims 62 and 64 depend on claim 61 and are believed to be allowable for at least the reasons claim 61 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 62 and 64 are respectfully requested.

Claims 1-6, 9-15, 17, 18, 20-29, 32-38, 40-43, 45-48, 50 and 51 have been rejected under 35 U.S.C. § 103(a) as being anticipated by Goldstone in view of Fedyk. The rejection is respectfully traversed.

Claim 1 recites a system for detecting and responding to an attack that includes a first device attached to a network and configured to detect an attack based on received traffic and create attack information. Claim 1 also recites that the first device is configured to forward the attack information to the network using a link state routing protocol or a path vector routing protocol. The Final Office Action admits that Goldstone does not disclose this latter feature, but states that Fedyk discloses a router layer and that the advantage of using the link state routing protocol is to rapidly pass on routing information to other routers in a network and points to col. 1, lines 25-40 of Fedyk for support (Final Office Action – page 4). The Final Office Action further states that it would have been obvious to improve on Goldstone "by using the link state

routing protocol method of Fedyk to provide a rapid response to DOS attack and thus reduce the time taken to recover from the attack" (Final Office Action – page 5). The applicant respectfully disagrees.

Fedyk at col. 1, lines 25-40 discloses that link state routing protocols are conventionally used to distribute routing information. The applicant respectfully submits that transmitting attack information using a link state routing protocol or a path vector routing protocol is significantly different than using a link state routing protocol in the manner it was intended to be used (i.e., to transmit routing information). As discussed in the applicant's specification at paragraph 73, for example, advertising attack information using such a routing protocol enables the attack information to be sent without having to design/use a special purpose flooding mechanism. This greatly simplifies the process for advertising attack information and enables the information to be communicated in an efficient manner. Neither Goldstone nor Fedyk, taken singly or in combination, discloses or suggests using a link state routing protocol or a path vector routing protocol to forward attack information, as required by claim 1.

In addition, the alleged motivation to modify Goldstone to forward attack information using a link state routing protocol (i.e., "to provide a rapid response to DOS attack and thus reduce the time taken to recover from the attack") is merely a conclusory statement providing an alleged benefit of the combination. No portion of either reference is pointed to as providing objective motivation for the combination. Such motivation does not satisfy the requirements of 35 U.S.C. § 103.

For at least these reasons, withdrawal of the rejection and allowance of claim 1 are respectfully requested.

Claims 2-6 and 9-13 are dependent on claim 1 and are believed to be allowable for at least the reasons claim 1 is allowable. In addition, these claims recite additional features not disclosed by the cited art.

For example, claim 2 recites that the first device comprises a firewall filter. Goldstone may disclose using a firewall to detect an attack. Goldstone, however, does not disclose that the firewall filter is able to forward attack information using a link state routing protocol or a path vector routing protocol, as required by claim 2. Fedyk, as discussed above, discloses that routers may use a link state routing protocol to communicate routing information. Fedyk, however, does not disclose that a firewall filter may use such a protocol. Further, as discussed in the applicant's specification at, for example, paragraph 80, conventional firewalls, such as the firewall in Goldstone, are not equipped to handle routing protocols. Therefore, even if routing protocols are known, it is not conventional or obvious for a firewall filter to communicate using either a link state routing protocol or a path vector routing protocol, as required by claim 2.

For at least these additional reasons, withdrawal of the rejection and allowance of claim 2 are respectfully requested.

Claims 14 and 25 recite features similar to, but not identical to claim 1. For reasons similar to those discussed above with respect to claim 1, the combination of Goldstone and

Fedyk does not disclose or suggest each of the features of claims 14 and 25. Accordingly, withdrawal of the rejection and allowance of claims 14 and 25 are respectfully requested.

Claims 15, 17, 18, 20-24, 26-29 and 32 variously depend on claims 14 and 25 and are believed to be allowable for at least the reasons claims 14 and 25 are allowable. Accordingly, withdrawal of the rejection and allowance of claims 15, 17, 18, 20-24, 26-29 and 32 are respectfully requested.

Claim 33 recites a method of detecting an attack that includes monitoring incoming traffic at a first device to detect an attack and generating attack information defining characteristics of the attack. Claim 33 also recites transmitting the attack information to a second device via a network using a link state routing protocol, a path vector routing protocol, a markup language protocol or a hypertext protocol.

Similar to the discussion above with respect to claim 1, neither Goldstone nor Fedyk discloses or suggest using link state routing protocol or a path vector routing protocol to transmit attack information. In addition, neither of these references discloses or suggests using a markup language protocol or a hypertext protocol to transmit attack information. Further, the applicants assert that the motivation to combine Goldstone and Fedyk does not satisfy the requirements of 35 U.S.C. § 103 for the reasons discussed above with respect to claim 1.

For at least these reasons, the combination of Goldstone and Fedyk does not disclose or suggest each of the features of claim 33. Accordingly, withdrawal of the rejection and allowance of claim 33 are respectfully requested.

Claims 34-38 and 40-42 depend on claim 33 and are believed to be allowable for at least the reasons claim 33 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 34-38 and 40-42 are respectfully requested.

Claim 43 recites features similar to, but not identical to claim 33. For reasons similar to those discussed above with respect to claim 33, the combination of Goldstone and Fedyk does not disclose or suggest each of the features of claim 43. Accordingly, withdrawal of the rejection and allowance of claim 43 are respectfully requested.

Claims 45-48, 50 and 51 depend on claim 43 and are believed to be allowable for at least the reasons claim 43 is allowable. Accordingly, withdrawal of the rejection and allowance of claims 45-48, 50 and 51 are respectfully requested.

Claims 19, 30, 31 and 49 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Goldstone in view of Fedyk and further in view of Nguyen et al. (U.S. Patent Publication No. 2002/0016926; hereinafter Nguyen). The rejection is respectfully traversed.

Claims 19, 30, 31 and 49 variously depend on claims 14, 25 and 43. These claims are believed to be allowable for at least the reasons their respective independent claims are allowable. Nguyen do not remedy the deficiencies in Goldstone and Fedyk discussed above with respect to claims 14, 25 and 43. Accordingly, withdrawal of the rejection and allowance of claims 19, 30, 31 and 49 are respectfully requested.

CONCLUSION

In view of the foregoing remarks, the applicant respectfully requests withdrawal of the outstanding rejections and the timely allowance of this application. In the event that the application is not allowed, the applicant respectfully requests withdrawal of the finality of the current Office Action for the reasons discussed above.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /Glenn Snyder/
Glenn Snyder
Reg. No. 41,428

Date: July 24, 2006

11350 Random Hills Road
Suite 600
Fairfax, VA 22030
Telephone: (571) 432-0800
Facsimile: (571) 432-0808